

Remarks

Claims 7 and 86 are amended. Claims 1, 3-14, 16-45, 47-52, 72-77 and 79-92 are pending in the application. Reconsideration of the rejections and objections at an early date is requested.

Claims 7 and 86 have been amended to correct typographical errors.

Claims 1-4, 6-12, 14, 16-32, 34-37, 43-45, 47, 50-52, 72-77, 79-82, 84-90 & 92 were rejected under 35 U.S.C. 103(a) as being unpatentable over Ice (U.S. Patent Number 6,598,031) in view of Robinson (U.S. Publication No. 2003/0061172). The examiner did not include in this list claims 48 and 49, but it seems apparent from the text of the rejection that these claims were also rejected on this basis.

Claims 3-5, 33, 38-42, 83 & 91 were rejected under 35 U.S.C. 103(a) as being unpatentable over Ice in view of Robinson and in further view of Official Notice.

Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ice in view of Robinson and in further view of Lapsley et al. US 2001/0000535.

The basis of the rejection is that *Ice* discloses all of the features of claims 1, 48, 49 & 50, except registering a user and checking for sufficient funds, which the examiner again suggests is disclosed in the abstract and col. 4, lines 54-57, of *Robinson*. The examiner contends that it would have been obvious to combine the teachings of these references, thereby rendering the invention obvious. Applicant respectfully disagrees for the following reasons.

Ice describes a computer terminal configured to facilitate the generation and transmission of encrypted information. The terminal receives a credit card number from the card (or a debit card number and further receives a PIN entered on a keypad). The card number is encrypted by an encryption unit that has a serial number. The encrypted credit card number and the serial number (and billing address) are sent to a payment server. The payment server has a database in

which is stored cryptograms associated with each serial number. The payment server generates a single use credit card number, which is stored in a data structure within the database along with the information received from the personal computer (i.e. the serial number and the unencrypted credit card number). The single use credit card number is returned to the personal computer.

The single use credit card number is provided to a merchant web site when a transaction is desired. The merchant uses the single use credit card number as a normal credit card number, by sending it to a gateway server. The gateway server recognizes the single use credit card number as being from the payment server and transmits the single use credit card number to the payment server. The payment server then compares the single use credit card number with (those in) the database and determines whether it is in the database. The serial number associated with the single use number is retrieved and this is then used to retrieve the credit card number sent by the personal computer. The credit card number is then returned to the gateway server and the rest of the process occurs in a conventional way.

It is respectfully submitted that *Ice* does not contain a disclosure of the all of the features said to be present by the examiner. It is apparent that the examiner has equated the single use transaction request identification (of the claim) with the single use credit card number (of the reference). The transaction manager (of the claim) seems to have been equated to the payment server (of the reference). Because the single use credit card number has been equated to the single use transaction request identification it can not also be the received user identifier (of the claim). While the address may be regarded as a user identifier, it is not received by the payment server (or the gateway server) in a payment request as required by claim 1 (and is therefore not the "received user identifier" referred to in the claim).

Specifically *Ice* does not disclose:

"receiving at the transaction manger a payment request comprising a received user identifier, a value and information for making a fund transfer of the value from the registered user identified by the received user identifier to an identified recipient, the payment request also including a received transaction request identification".

This is because the gateway server receives the payment request (col. 5, lines 32-36: "the web server transmits the (single use credit card) number to the gateway server in a manner conventionally used for processing credit card orders"). The payment server receives only the single use credit card number (col. 5, lines 46-47: "the gateway server then transmits the single-use credit card number to the payment server") and replaces the single use credit card number with the actual credit card number (col. 5, lines 57-60: "this decoded data is returned to the gateway server which provided the single-use credit card number, providing the actual number of the credit card in a conventional way"), so that the gateway server can proceed with the transaction in a conventional way (col. 5, lines 61-65).

Additionally the payment request received by the gateway server only has the single use credit card number in place of the actual credit card number and the other conventional information in a credit card payment. This would be the value and the identity of the merchant. Specifically it does not contain an identifier of the user, because the actual credit card number (or some other identifier of the user) is not sent and well as the single use credit card number.

The gateway server of *Ice* does not:

"(determine) the validity of the received payment request by checking the validity of the received transaction request identification and whether the received transaction request identification is stored in a relationship with the received user identification".

Instead the payment server checks the validity of the single use single use credit card number and whether the received transaction request identification is stored in a relationship with the serial number and in turn with the decrypted credit card number and address, (neither of which were received in the payment request). Therefore the payment server also does not:

"(determine) the validity of the received payment request by checking the validity of the received transaction request identification and whether the received transaction request identification is stored in a relationship with the received user identification".

In addition while the gateway server inherently must receive a value as part of a processing of a credit card order, the payment server does not receive the value and does not need to receive a value because it only receives the single use credit card number in this phase of the transaction (col. 5, lines 61-65).

It is the gateway server that proceeds with a conventional credit card transaction (after the payment server has substituted the single-use credit card number with the actual credit card number) and not the payment server. Therefore, it is the gateway server and not the payment server that:

“(receives) at the transaction manager apparatus (the payment server) confirmation of the transfer from the financial institution when the transfer is performed”

(See col. 5, line 65 – col. 6, line 1: “upon subsequent receipt of the approval the gateway server provides an indication to the merchant’s web site server that the transaction has been approved”).

To reiterate, the received user identifier is distinct from the single use transaction request identification (of the claim) or the single use credit card number (of the reference). Further, at least the absence of the received user identifier in the payment request results in claim 1 comprising at least the new feature of *“receiving at the transaction manger a payment request comprising a received user identifier...”*. Because the prior art does not teach or suggest this feature, as well as the other features mentioned above, claim 1 is not obvious.

There are other differences in the dependent claims, some of which are explained below.

With regard to claim 14, this requires the payment request to further comprise a component provided by the registered user and the transaction manager apparatus receives the user provided component from the user independently from and before receiving the purchase request, and storing of the user provided component in the storage in a relationship with the identifier of the registered user. This is not disclosed in *Ice* despite the assertion that it is disclosed by the user

swiping the card, because the user provided component is not provided in the payment request. Only the single use credit card number (the value and merchant ID) are provided in payment request.

With regard to claim 16, this requires comparing the user provided component received in the payment request with the stored user provided component to determine the validity of the payment request. Since the payment request does not include the user provided component this comparison can not occur.

Claim 17 requires the user provided component comprise a secret identification of the user known to the registered user. Ice discloses providing a PIN to the payment server, but this is a precursor step and not part of a payment request.

Claim 18 requires a transaction limit and with a transaction limit override password. While Robinson may describe a transaction limit, there is no disclosure of a transaction limit override password.

Claim 26 requires combining the transaction request identification and the user provided component by hatching. Ice makes no disclosure of hatching.

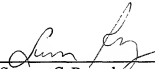
Claim 28 requires a user provided component that comprises a secret identification of the user known to the registered user and recorded in the financial institution. Again while providing a PIN to the payment server is disclosed as a precursor step, there is no disclosure of the PIN being provided in a payment request.

In view of the comments above, Applicant respectfully requests an allowance of the pending claims at an early date.

ATTORNEY DOCKET NO. 26016.0004U1
APPLICATION NO. 10/506,739

A Credit Card Payment submitted via EFS-Web authorizing payment in the amount of \$65.00 for a small entity under 37 C.F.R. § 1.17(a)(1) for a one month extension of time, a Request for Extension of Time. This fee is believed to be correct, however, the Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 14-0629.

Respectfully submitted,



Sumner C. Rosenberg
Registration No. 28,753

BALLARD SPAHR LLP
Customer Number 23859
(678) 420-9300 Phone
(678) 420-9301 Fax